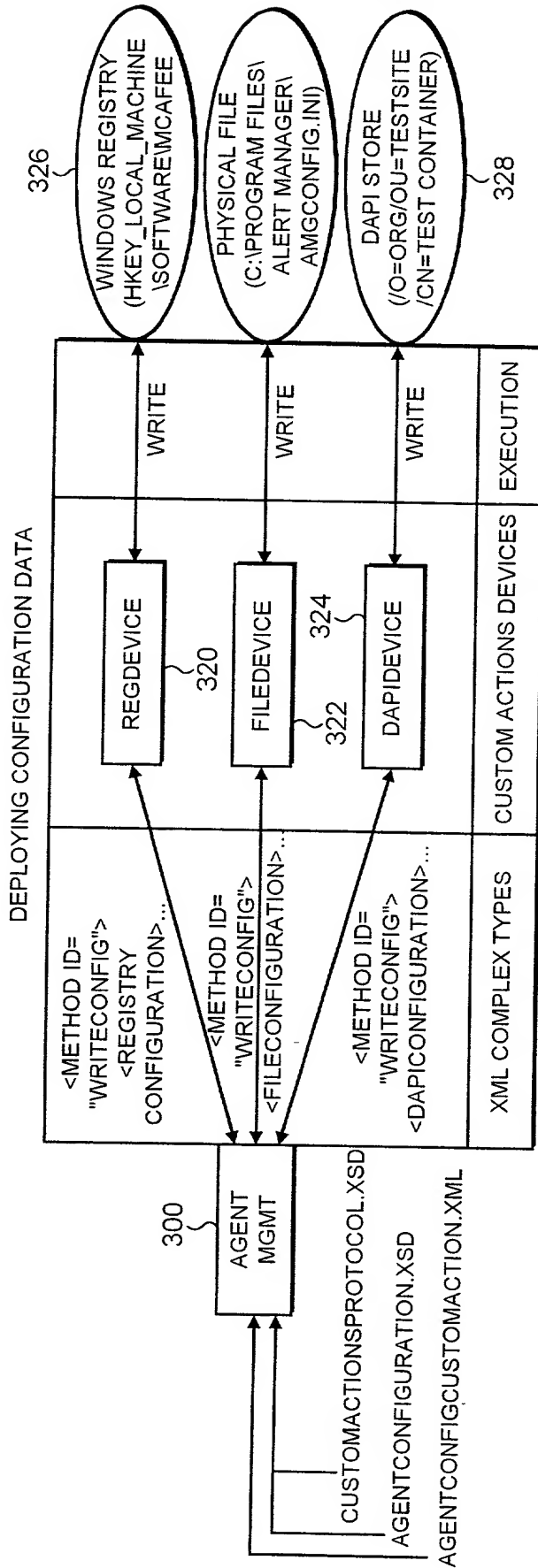


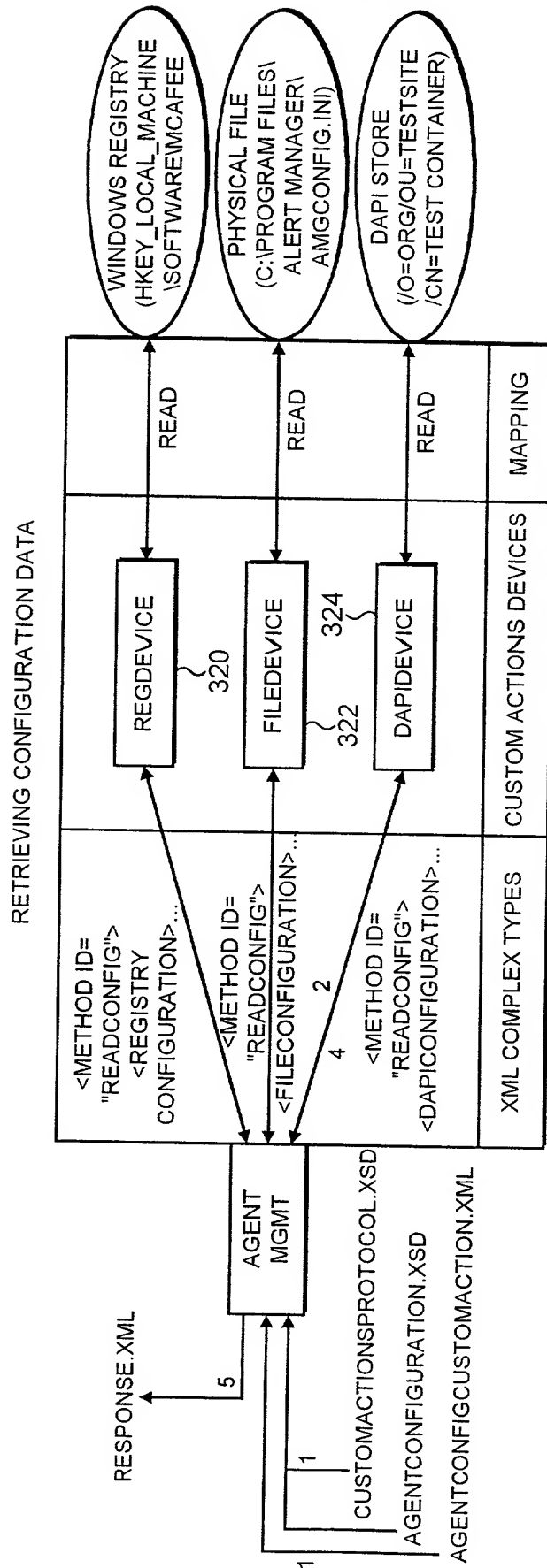
- 1) REQUEST XML FILE IS PASSED TO AGENT MGMT CONTAINING COMPLEX TYPES
- 2) THE COMPLEX TYPE <METHOD> DESCRIBES THE METHOD TO EXECUTE AND ITS PARAMETERS EACH <METHOD> IS PASSED TO THE CORRESPONDING CUSTOM ACTIONS DEVICE
- 3) CUSTOM ACTIONS DEVICES EXECUTE THE FUNCTIONS AND PACK THE RESULT INTO XML COMPLEX TYPES
- 4) COMPLEX TYPES CONTAINING RESULT DATA ARE RETURNED TO AGENT MGMT
- 5) XML STREAM HAS BEEN PACKED AND IS RETURNED

FIG. 2



- 1) AGENT MGMT RECEIVES AGENTCONFIGCUSTOMACTION.XML
- 2) .XML FILE IS VALIDATED AGAINST .XSD FILE(S) TO MAKE SURE VALID DATA IS WRITTEN
- 3) XML COMPLEX TYPES ARE SENT TO CUSTOM ACTIONS DEVICES, THE PARAMETERS CONTAINING THE CONFIGURATION DATA
- 4) CUSTOM ACTIONS DEVICES UPDATE THE CONFIG STORE THEY ARE RESPONSIBLE FOR
- 5) OPTIONALLY A RETURN VALUE CAN BE RETURNED AS A RESPONSE.XML FILE

FIG. 3



- 1) REQUEST XML FILE IS PASSED TO AGENT MGMT CONTAINING EMPTY REQUESTED COMPLEX TYPES
- 2) THE EMPTY COMPLEX TYPES ARE PASSED TO THE CUSTOM ACTIONS DEVICE
- 3) COMPLEX TYPES ARE FILLED BY MAPPING REQUIRED DATA FROM STORE
- 4) COMPLEX TYPES CONTAINING DATA ARE RETURNED TO AGENT MGMT
- 5) XML STREAM HAS BEEN PACKED AND IS RETURNED

FIG. 4

5 / 25

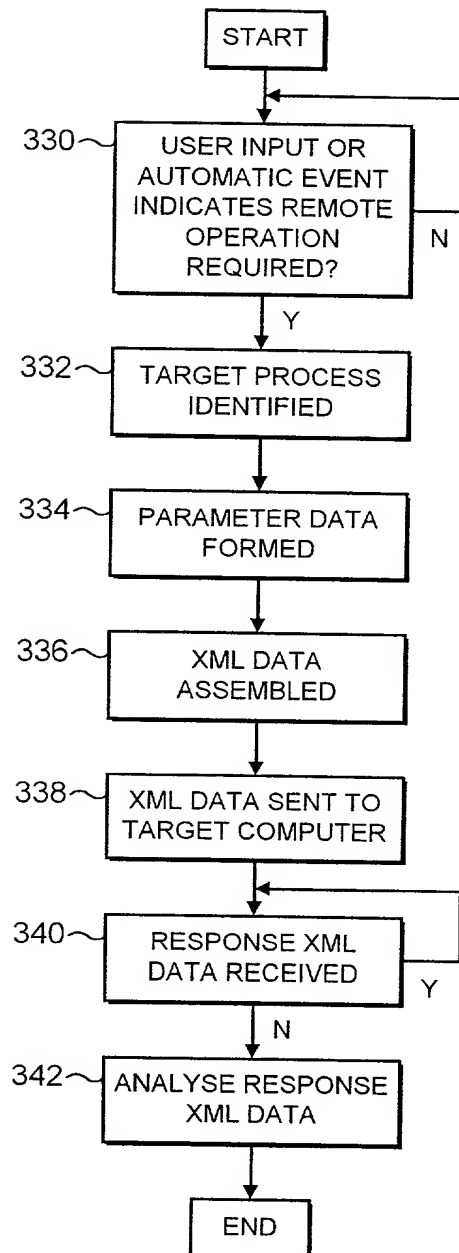


FIG. 5

205990-0242007

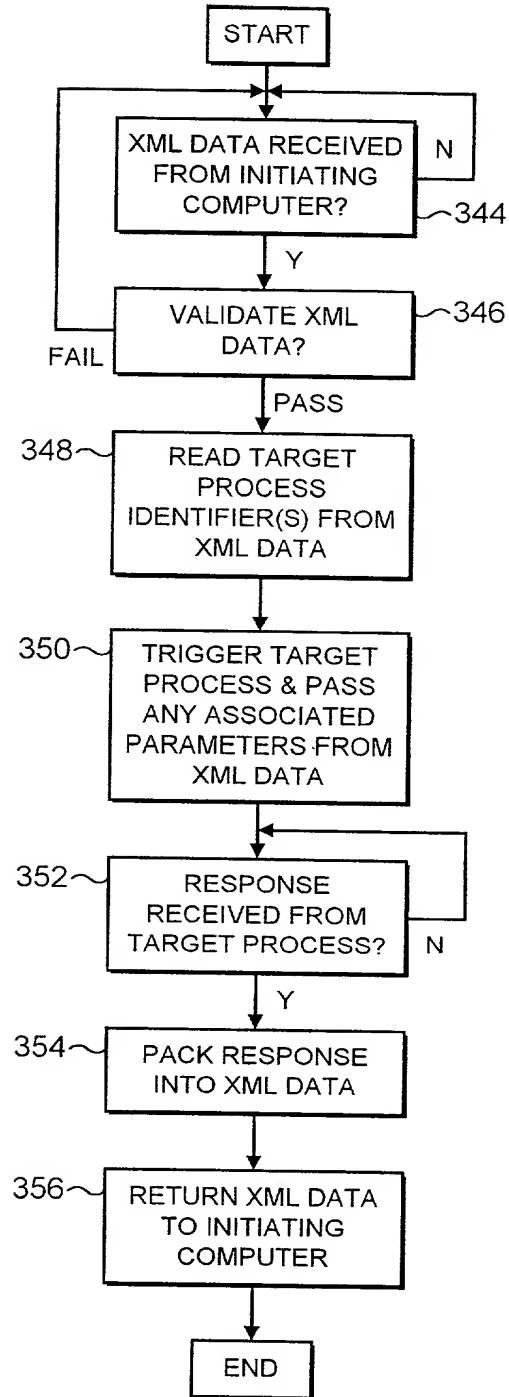


FIG. 6

2009420-060502

7 / 25

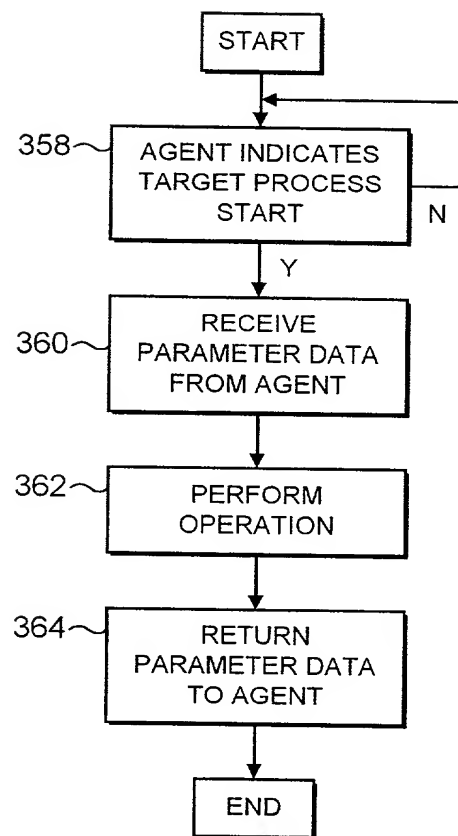


FIG. 7

20092420.060502

200902426001

PROTOCOL SPECIFICATION	
<CONTROL DATA>	CONTAINS AGENT SPECIFIC CONTROL DATA LIKE VERSION INFORMATION, THE COMMAND TO EXECUTE AND COMPUTER INFORMATION SENDING THE CUSTOM ACTIONS INFORMATION
<COMMAND>	THE COMMAND FIELD COULD BE USED TO EASILY DETERMINE IF DATA IS GOING TO BE RETRIEVED (REQUEST CUSTOM ACTION) OR RETURNED AFTER THE ACTION HAS BEEN EXECUTED (RESPOND TO CUSTOM ACTION) - OPTIONAL
<SERVER>	COMPUTER INFORMATION OF THE SENDER. IF THE AGENT IS ABLE TO PROCESS REQUESTS IN PARALLEL AND ASYNCHRONOUSLY, THIS INFORMATION IS USEFUL. THE SIMPLEST FORM OF THIS FIELD CONTAINS THE COMPUTER NAME
<CUSTOM ACTIONS>	ANY NUMBER OF CUSTOM ACTION COM SERVERS OR DLLS OR EXECUTABLES REQUIRED FOR THE TASKS ARE LISTED WITHIN THE CUSTOM ACTIONS
ID	THE ID SPECIFIES A CLSID IF THE CUSTOM ACTION METHOD IS CONTAINED IN A COM SERVER OR THE PATH TO A DLL/EXE FILE IF A LIBRARY OR AN EXECUTABLE IMPLEMENTS THE METHOD TO EXECUTE. IF A CLSID IS SPECIFIED, THE FOLLOWING <INTERFACE> COMPLEX TYPE IS REQUIRED TO SPECIFY THE INTERFACE OF THE COM SERVER CONTAINING THE METHOD TO EXECUTE. OTHERWISE <INTERFACE> IS NOT REQUIRED AND ANY NUMBER OF <METHOD> TYPES FOLLOW IMMEDIATELY
<INTERFACE>	ONLY REQUIRED IF THE <METHOD> IS IMPLEMENTED IN A COM SERVER
ID	THE INTERFACE IDENTIFIER OF THE COM SERVER (IID)
<METHOD>	ANY NUMBER OF METHODS IMPLEMENTED IN THE CUSTOM ACTION DEVICE
ID	THE METHOD NAME. IN CASE OF A COM SERVER, THIS IS THE METHOD NAME OF THE COM INTERFACE, ELSE THIS DENOTES THE NAME OF AN EXPORTED FUNCTION OR E.G. A COMMAND LINE PARAMETER OF AN EXECUTABLE
<PARAMETER>	ANY NUMBER OF PARAMETERS REQUIRED FOR THE METHOD. THIS INCLUDES REQUESTED OUT PARAMETERS, WHICH ARE LISTED, BUT DON'T CONTAIN DATA AND INOUT PARAMETERS WHICH HAVE A DIFFERENT VALUE ON RESPONSE THAN ON REQUEST
ID	THE NAME OF THE PARAMETER
TYPE	CAN BE ANY STANDARD XML DATATYPE
INOUT	POSSIBLE VALUES ARE 'IN' AND 'INOUT'. SPECIFIES IF THE PARAMETER IS REQUESTED, PASSED TO THE FUNCTION OR PASSED TO THE FUNCTION FOR MODIFICATION
<ANY>	ANY OTHER NON STANDARD XML DATATYPE CAN FOLLOW

FIG. 8

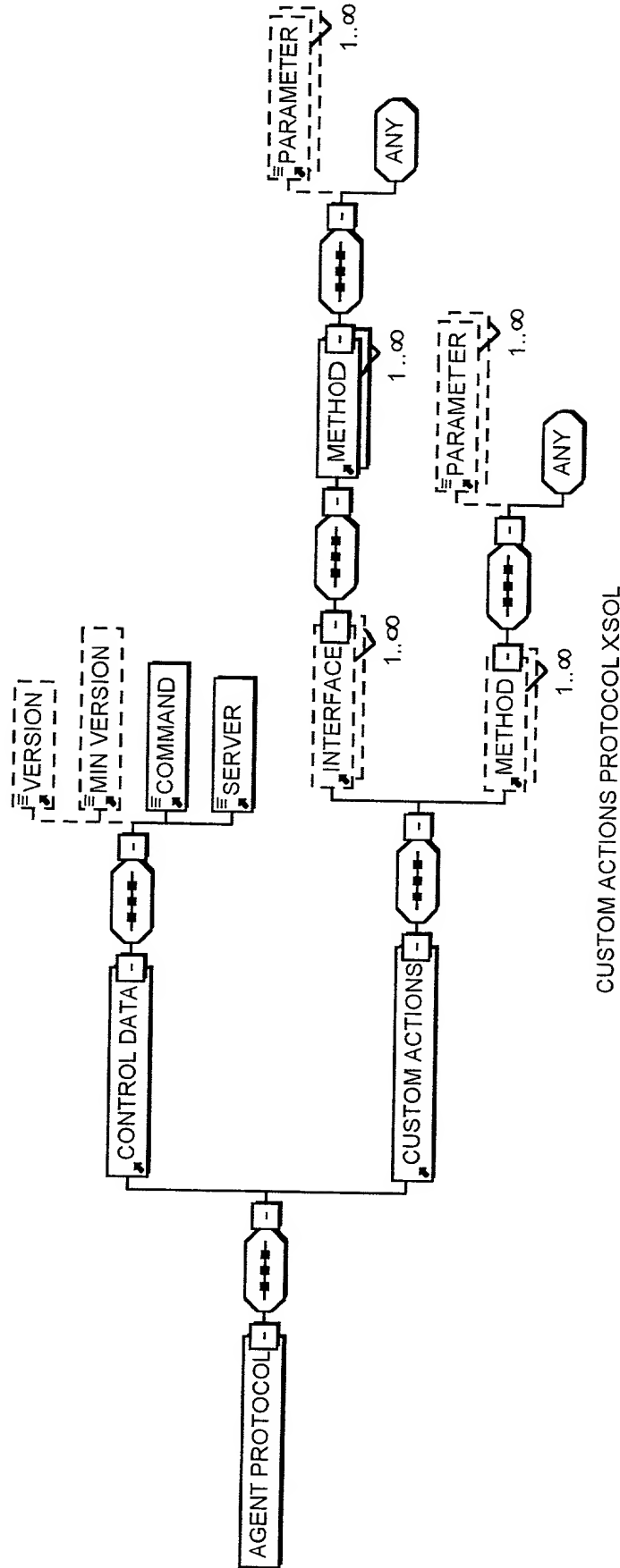


FIG. 9

10 / 25

```
<?xml version="1.0" ?>
- <AgentProtocol xmlns="http://www.nai.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.nai.com CustomActionsProtocol.xsd">
- <ControlData>
  <Version>0x01000001</Version>
  <MinVersion>0x01000001</MinVersion>
  <Command>RequestCustomAction</Command>
  <Server>ned1wnts2ke</Server>
</ControlData>
- <CustomActions
  id="<AGENT_INSTALLED_DIR>\\CustomActionsLibrary\\CustAct1.dll">
- <Method id="GetRegStringValue">
  <Parameter id="Key" type="xs:string"
    inout="in"><AGENT_INSTALLED_REGKEY></Parameter>
  <Parameter id="Valuename" type="xs:string"
    inout="in">AgentVersion</Parameter>
  <Parameter id="Result" type="xs:string" inout="out" />
</Method>
</CustomActions>
- <CustomActions id="{06E0062A-5069-4793-ACED-F80BE1BBC4AF}">
- <Interface id="{C9E1CC03-8007-412A-8F5D-532C57DF4482}">
- <Method id="ExecuteSilentInstallation">
  <Parameter id="ProductName" type="xs:string"
    inout="in">TestInstallProduct</Parameter>
  <Parameter id="ProductVersion" type="xs:decimal"
    inout="in">0x01000001</Parameter>
  <Parameter id="Location" type="xs:string"
    inout="in">c:\InstallImages</Parameter>
  <Parameter id="Result" type="xs:string" inout="out" />
</Method>
</Interface>
- <Interface id="{C9E1CC03-8007-412A-8F5D-532C57DF4482}">
- <Method id="GetSystemDirectory">
  <Parameter id="Directory" type="xs:string" inout="out" />
  <Parameter id="Result" type="xs:decimal" inout="out" />
</Method>
</Interface>
</CustomActions>
- <CustomActions id="{06E0062B-5069-4793-ACED-F80BE1BBC4AF}">
- <Interface id="{A000CC03-8007-412A-8F5D-532C57DF4482}">
- <Method id="TriggerEvent">
  <Parameter id="EventID" type="xs:decimal"
    inout="in">1000</Parameter>
  <Parameter id="EventDescription" type="xs:decimal"
    inout="in">The event %EventID% has been triggered by %
    USERNAME% on computer %COMPUTERNAME%. The %
    FILENAME% file is infected with %VIRUSNAME%. This has
    been detected by engineversion %ENGINEVERSION%
    datversion %DATVERSION%.</Parameter>
  <Parameter id="COMPUTERNAME" type="xs:string"
    inout="in">sourcecomputer</Parameter>
  <Parameter id="USERNAME" type="xs:string"
    inout="in">sourceuser</Parameter>
  <Parameter id="FILENAME" type="xs:string"
    inout="in">kernel32.dll</Parameter>
  <Parameter id="VIRUSNAME" type="xs:string"
```

CUSTOM ACTIONS PROTOCOL RESP XML

FIG. 10A

205990.024202

2009-02-03 10:00:00

```
inout="in">Nimbda</Parameter>
  <Parameter id="ENGINEVERSION" type="xs:decimal"
    inout="in">0x04005001</Parameter>
  <Parameter id="DATVERSION" type="xs:decimal"
    inout="in">0x07003009</Parameter>
  <Parameter id="Result" type="xs:string" inout="out" />
</Method>
</Interface>
</CustomActions>
</AgentProtocol>
```

CUSTOM ACTIONS PROTOCOL REQ XML

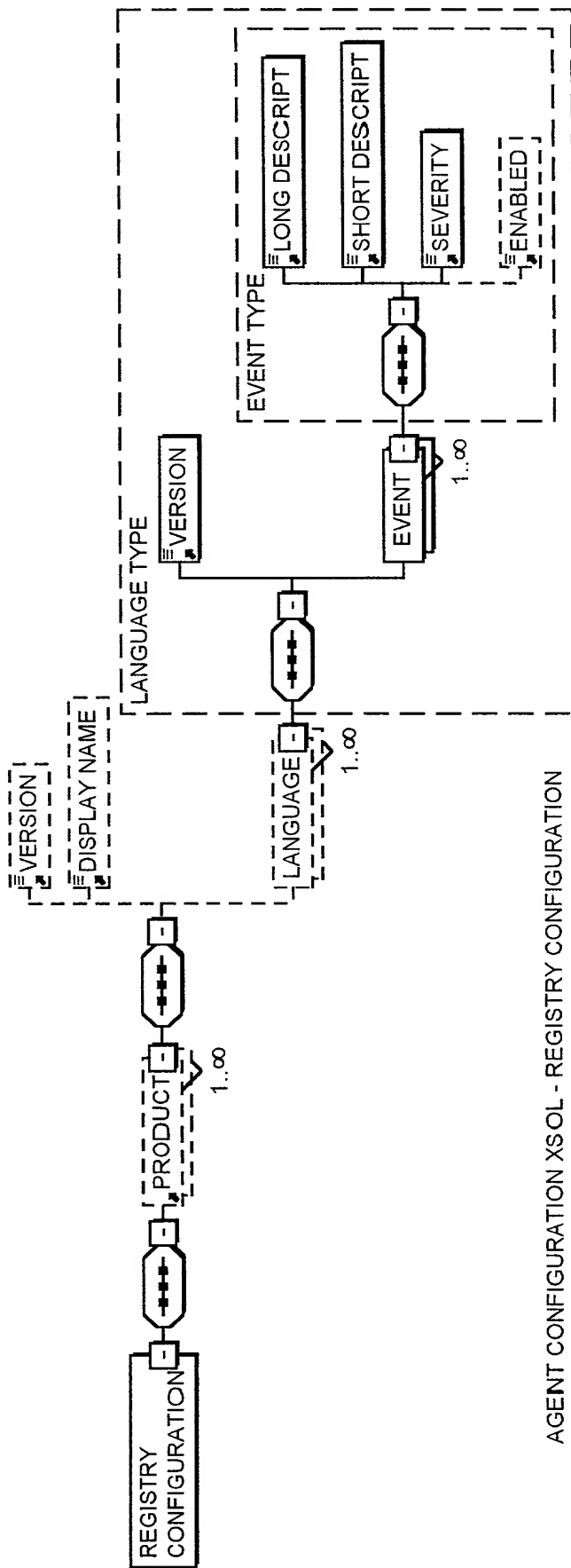
FIG. 10B

12 / 25

```
<?xml version="1.0" ?>
- <AgentProtocol xmlns="http://www.nai.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.nai.com CustomActionsProtocol.xsd">
- <ControlData>
  <Version>0x01000001</Version>
  <MinVersion>0x01000001</MinVersion>
  <Command>RespondToCustomAction</Command>
  <Server>ned1wnts2ke</Server>
</ControlData>
- <CustomActions
  id="<AGENT_INSTALLED_DIR>\\CustomActionsLibrary\\CustAct1.dll">
- <Method id="GetRegStringValue">
  <Parameter id="Result" type="xs:string"
    inout="out">5.0.1.10</Parameter>
</Method>
</CustomActions>
- <CustomActions id="{06E0062A-5069-4793-ACED-F80BE1BBC4AF}">
- <Interface id="{C9E1CC03-8007-412A-8F5D-532C57DF4482}">
  - <Method id="ExecuteSilentInstallation">
    <Parameter id="Result" type="xs:string" inout="out">Error: Invalid
      Image path specified.</Parameter>
  </Method>
</Interface>
- <Interface id="{C9E1CC03-8007-412A-8F5D-532C57DF4482}">
  - <Method id="GetSystemDirectory">
    <Parameter id="Directory" type="xs:string"
      inout="out">C:\Winnt\System32</Parameter>
    <Parameter id="Result" type="xs:decimal"
      inout="out">0</Parameter>
  </Method>
</Interface>
</CustomActions>
- <CustomActions id="{06E0062B-5069-4793-ACED-F80BE1BBC4AF}">
- <Interface id="{A000CC03-8007-412A-8F5D-532C57DF4482}">
  - <Method id="TriggerEvent">
    <Parameter id="Result" type="xs:string" inout="out">Event sent to
      testcomputer2</Parameter>
  </Method>
</Interface>
</CustomActions>
</AgentProtocol>
```

CUSTOM ACTIONS PROTOCOL RESP XML

FIG. 11



AGENT CONFIGURATION XSD - REGISTRY CONFIGURATION

FIG. 12

14 / 25

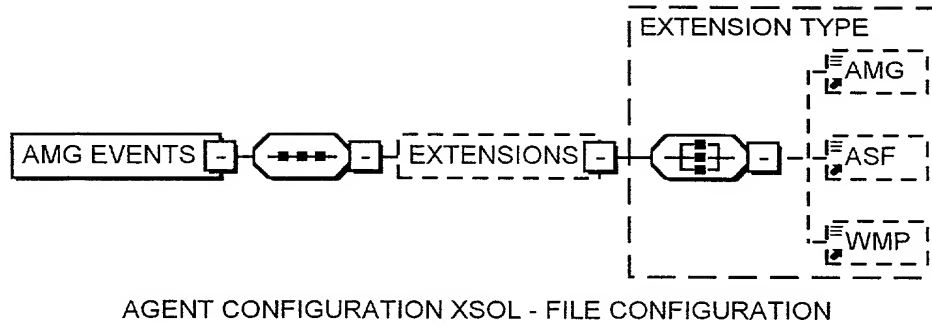
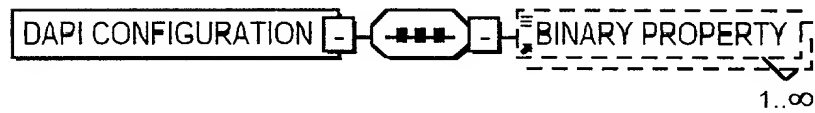


FIG. 13



AGENT CONFIGURATION XSOL - DAPI CONFIGURATION

FIG. 14

205990-02426001

15 / 25

```
<?xml version="1.0" ?>
- <AgentProtocol xmlns="http://www.nai.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.nai.com CustomActionsProtocol.xsd
  http://www.nai.com AgentConfiguration.xsd">
- <ControlData>
  <Version>0x01000001</Version>
  <MinVersion>0x01000001</MinVersion>
  <Command>RequestCustomAction</Command>
  <Server>ned1wnts2ke</Server>
</ControlData>
- <CustomActions id="RegistryMapping.dll">
- <Method id="WriteConfig">
  - <RegistryConfiguration
    id="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee">
  - <Product id="Alert Manager">
    <Version>0x04070000</Version>
    <DisplayName>Alert Manager 4.7</DisplayName>
  - <Language id="0407">
    <Version>0x01000002</Version>
  - <Event id="1">
    <LONGDESCRIPT>Das ist eine Test-Nachricht von Alert
      Manager.</LONGDESCRIPT>
    <SHORTDESCRIPT>Testing</SHORTDESCRIPT>
    <Severity>5</Severity>
    <Enabled>1</Enabled>
  </Event>
  </Language>
  - <Language id="0409">
    <Version>0x01000002</Version>
  - <Event id="1">
    <LONGDESCRIPT>This is an alert manager test
      messge.</LONGDESCRIPT>
    <SHORTDESCRIPT>Testing</SHORTDESCRIPT>
    <Severity>0</Severity>
    <Enabled>1</Enabled>
  </Event>
  - <Event id="2">
    <LONGDESCRIPT>Text of event 2.</LONGDESCRIPT>
    <SHORTDESCRIPT>Testing</SHORTDESCRIPT>
    <Severity>1</Severity>
  </Event>
  </Language>
  </Product>
  </RegistryConfiguration>
  </Method>
- <Method id="ReadConfig">
  <RegistryConfiguration
    id="HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\*" />
  </Method>
</CustomActions>
- <CustomActions id="INIFileMapping.dll">
- <Method id="WriteConfig">
  - <FileConfiguration id="C:\Program Files\Alert
    Manager\AMGConfig.ini">
  - <Extensions>
```

AGENT CONFIG CUSTOM ACTION XML

FIG. 15A

10092420.050502

10092420.050502

```
<amg>AMGConfig</amg>
<asf>MPEGVideo</asf>
<wmp>MPEGVideo2</wmp>
</Extensions>
</FileConfiguration>
</Method>
- <Method id="ReadConfig">
  <FileConfiguration id="C:\Program Files\Alert
    Manager\AMGConfig.ini" />
</Method>
</CustomActions>
- <CustomActions id="MAPIMapping.dll">
- <Method id="WriteConfig">
  - <DAPIConfiguration id="/O=org/OU=TestSite/CN=TestContainer">
    <BinaryProperty>0123456789ABCDEF00000</BinaryProperty>
  </DAPIConfiguration>
</Method>
- <Method id="ReadConfig">
  <DAPIConfiguration id="/O=org/OU=TestSite/CN=TestContainer" />
</Method>
</CustomActions>
</AgentProtocol>
```

AGENT CONFIG CUSTOM ACTION XML

FIG. 15B

17 / 25

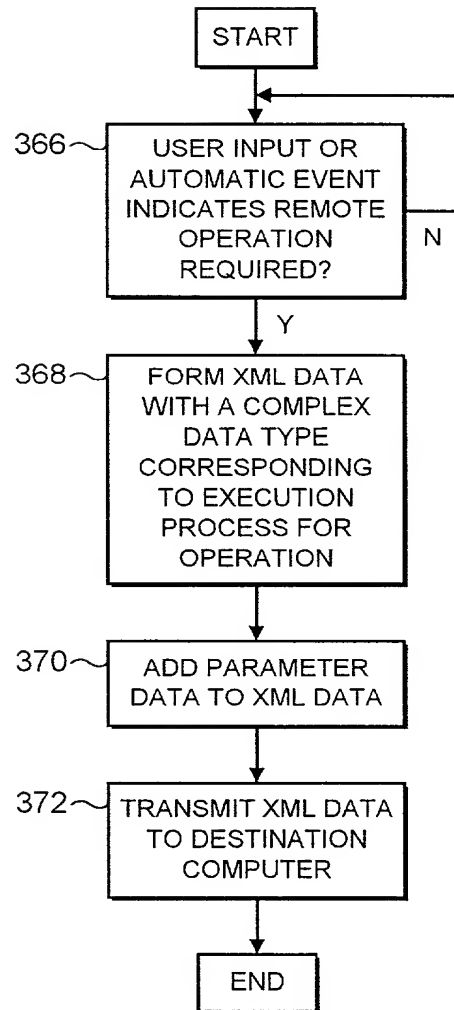


FIG. 16

18 / 25

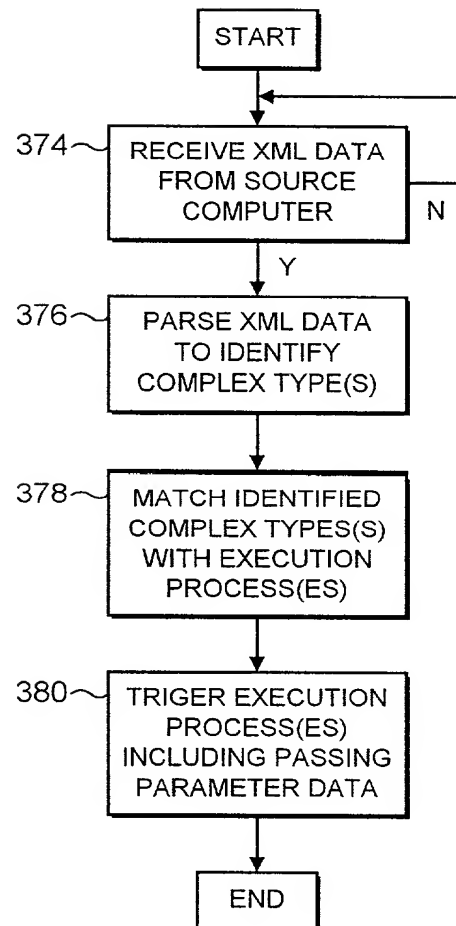
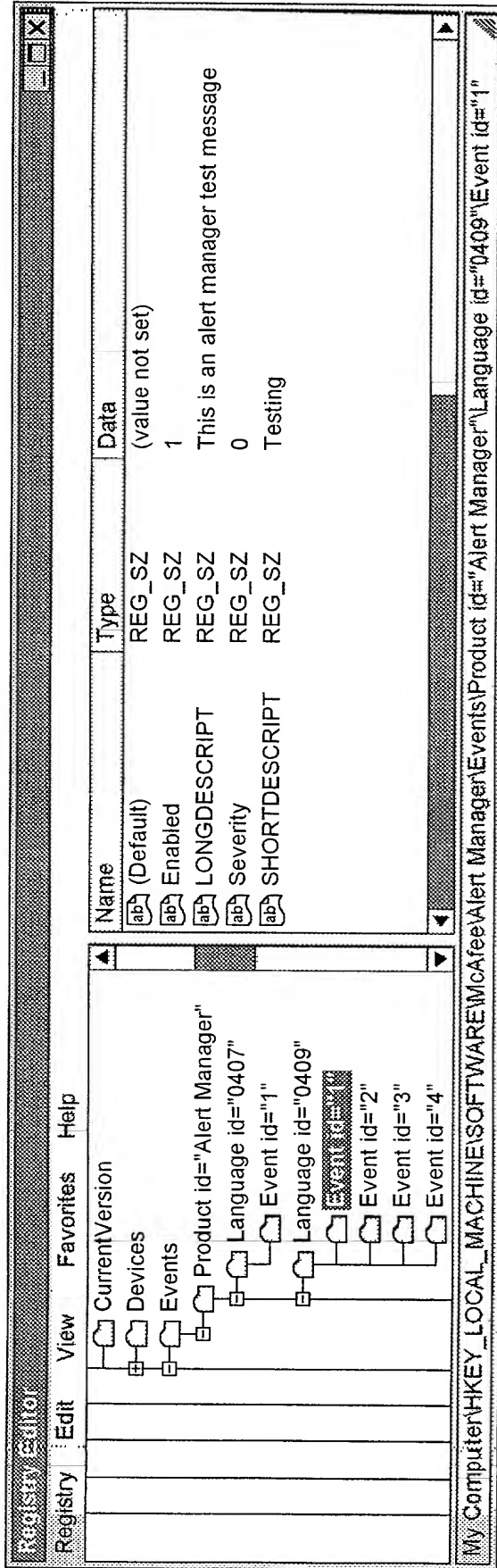


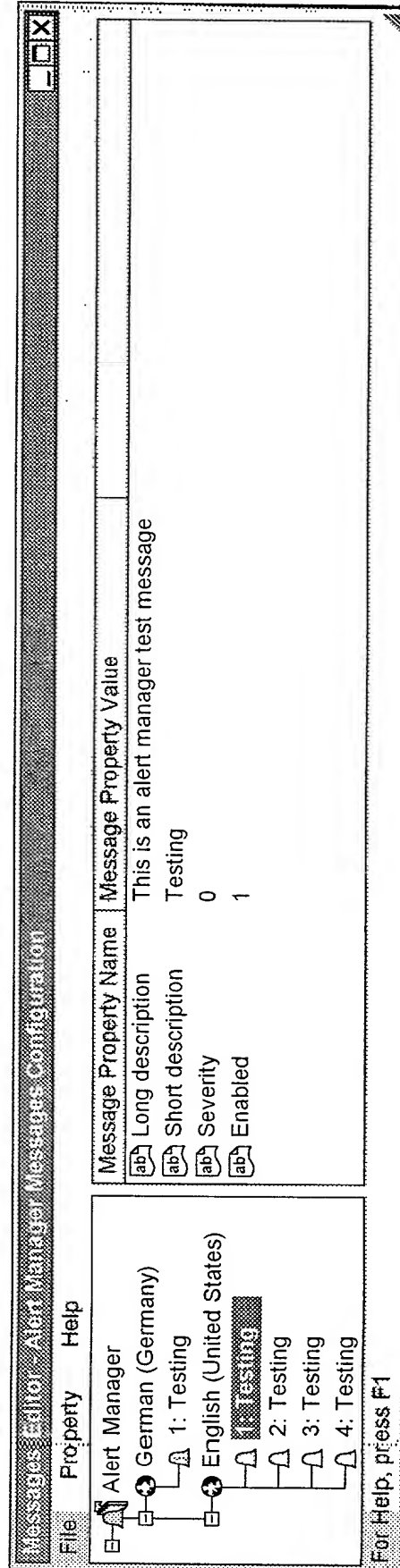
FIG. 17

205090" 0242600T

19 / 25



REGISTRY DATA FIG. 18



DOM DATA VIEW FIG. 19

20 / 25

```
<?xml version="1.0" ?>
- <AMGEvents xmlns="http://www.nai.com"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.nai.com AMGEvents.xsd">
- <Product id="Alert Manager">
  <Version>0x04070000</Version>
  <DisplayName>Alert Manager 4.7</DisplayName>
- <Language id="0407">
  <Version>0x01000002</Version>
  - <Event id="1">
    <LONGDESCRIPT>Das ist eine Test-Nachricht von Alert
      Manager.</LONGDESCRIPT>
    <SHORTDESCRIPT>Testing</SHORTDESCRIPT>
    <Severity>5</Severity>
    <Enabled>1</Enabled>
  </Event>
</Language>
- <Language id="0409">
  <Version>0x01000002</Version>
  - <Event id="1">
    <LONGDESCRIPT>This is an alert manager test
      messge.</LONGDESCRIPT>
    <SHORTDESCRIPT>Testing</SHORTDESCRIPT>
    <Severity>0</Severity>
    <Enabled>1</Enabled>
  </Event>
  - <Event id="2">
    <LONGDESCRIPT>Text of event 2.</LONGDESCRIPT>
    <SHORTDESCRIPT>Testing</SHORTDESCRIPT>
    <Severity>1</Severity>
  </Event>
  - <Event id="3">
    <LONGDESCRIPT>Text of event 3.</LONGDESCRIPT>
    <SHORTDESCRIPT>Testing</SHORTDESCRIPT>
    <Severity>1</Severity>
  </Event>
  - <Event id="4">
    <LONGDESCRIPT>Text of event 4.</LONGDESCRIPT>
    <SHORTDESCRIPT>Testing</SHORTDESCRIPT>
    <Severity>1</Severity>
  </Event>
</Language>
</Product>
</AMGEvents>
```

XML DATA

FIG. 20

20090909 024600

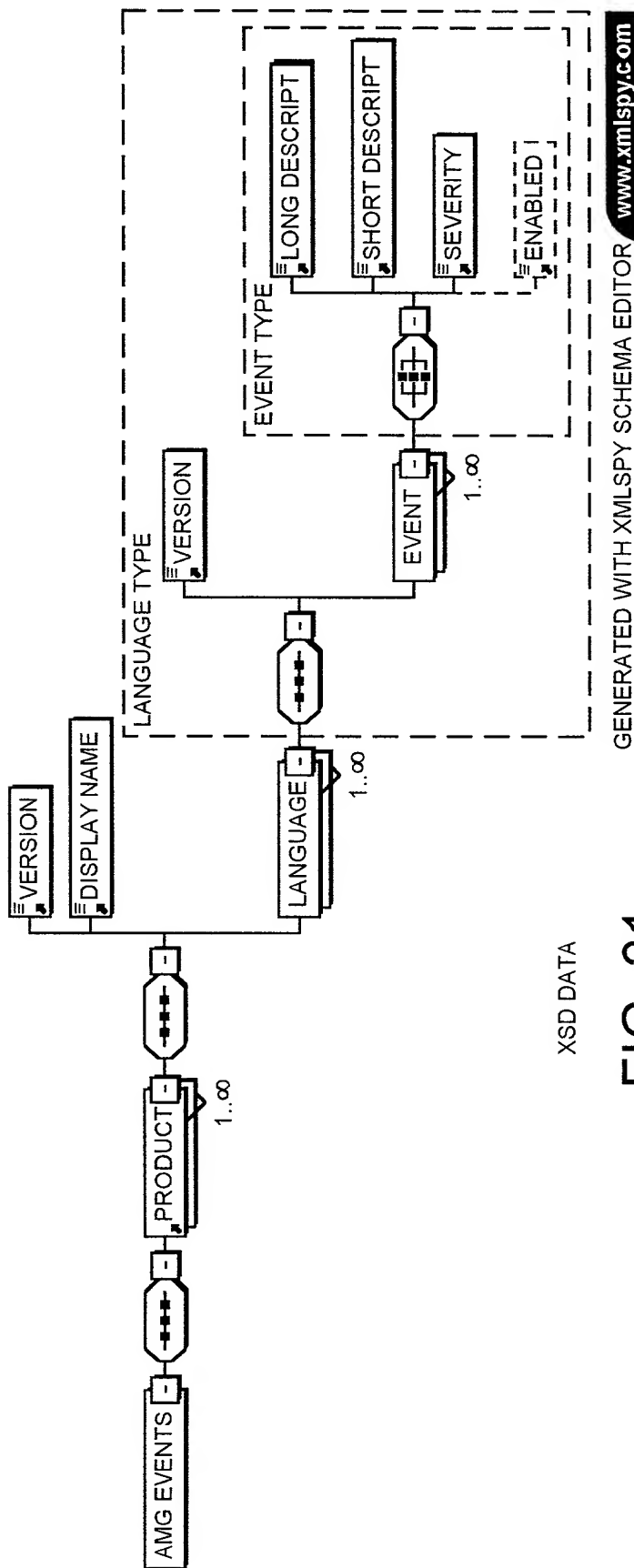


FIG. 21

22 / 25

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- edited with XML Spy v4.3.1 U (http://www.xmlspy.com) by Napalm
(Napalm) -->
- <xs:schema targetNamespace="http://www.nai.com"
  xmlns="http://www.nai.com"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">
  <xs:element name="DisplayName" type="xs:string" />
  <xs:element name="Enabled" type="xs:boolean" />
  - <xs:complexType name="EventType">
    - <xs:all>
      <xs:element ref="LONGDESCRIPT" />
      <xs:element ref="SHORTDESCRIPT" />
      <xs:element ref="Severity" />
      <xs:element ref="Enabled" minOccurs="0" />
    </xs:all>
    <xs:attribute name="id" type="xs:string" use="required" />
  </xs:complexType>
  - <xs:complexType name="LanguageType">
    - <xs:sequence>
      <xs:element ref="Version" />
      <xs:element name="Event" type="EventType"
        maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="id" type="xs:string" use="required" />
  </xs:complexType>
  - <xs:element name="Product">
    - <xs:complexType>
      - <xs:sequence>
        <xs:element ref="Version" />
        <xs:element ref="DisplayName" />
        <xs:element name="Language" type="LanguageType"
          maxOccurs="unbounded" />
      </xs:sequence>
      <xs:attribute name="id" type="xs:string" use="required" />
    </xs:complexType>
  </xs:element>
  - <xs:element name="AMGEvents">
    - <xs:complexType>
      - <xs:sequence>
        <xs:element ref="Product" maxOccurs="unbounded" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="LONGDESCRIPT" type="xs:string" />
  <xs:element name="SHORTDESCRIPT" type="xs:string" />
  <xs:element name="Severity" type="xs:string" />
  <xs:element name="Version" type="xs:string" />
</xs:schema>
```

XSD DATA

FIG. 22

10092420.060302

23 / 25

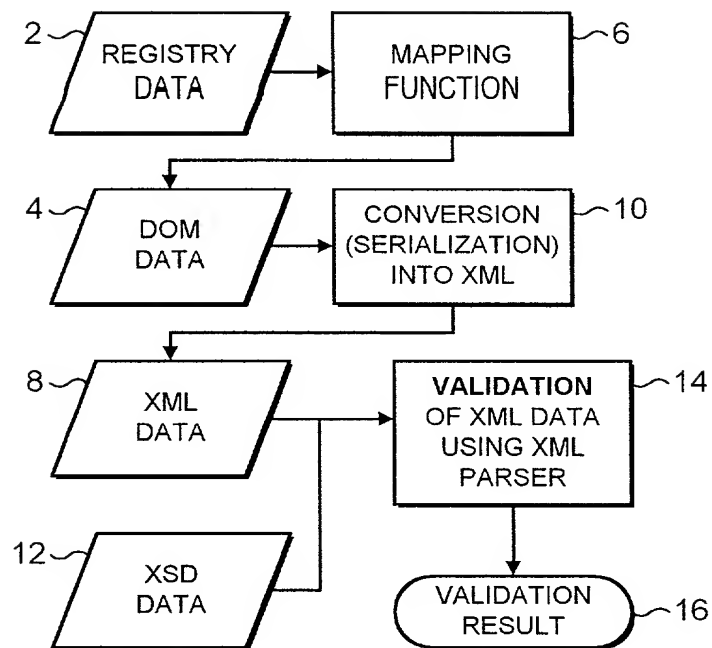


FIG. 23

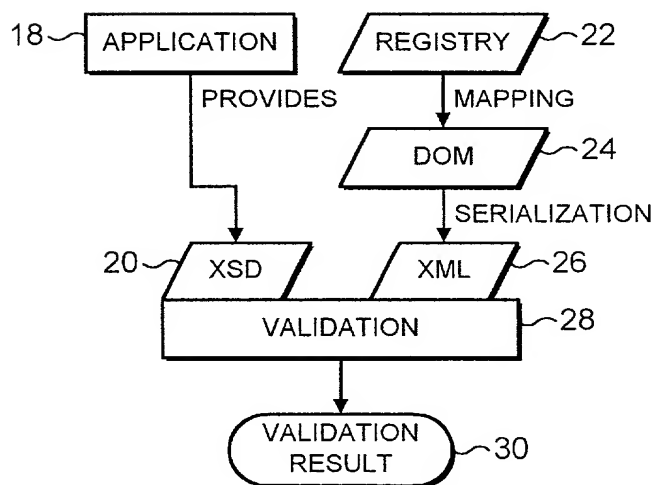


FIG. 24

20250902 024250T

24 / 25

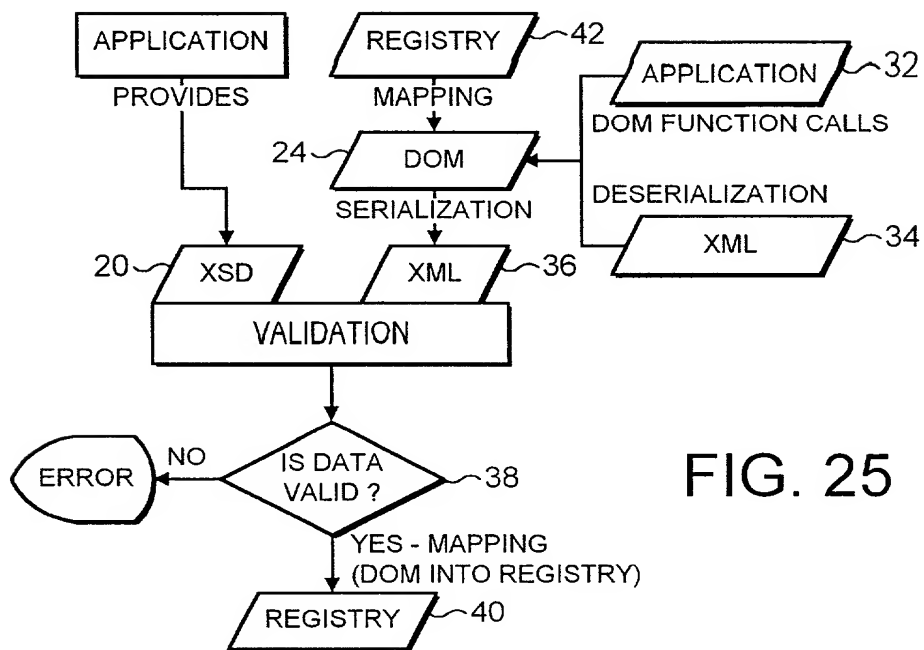


FIG. 25

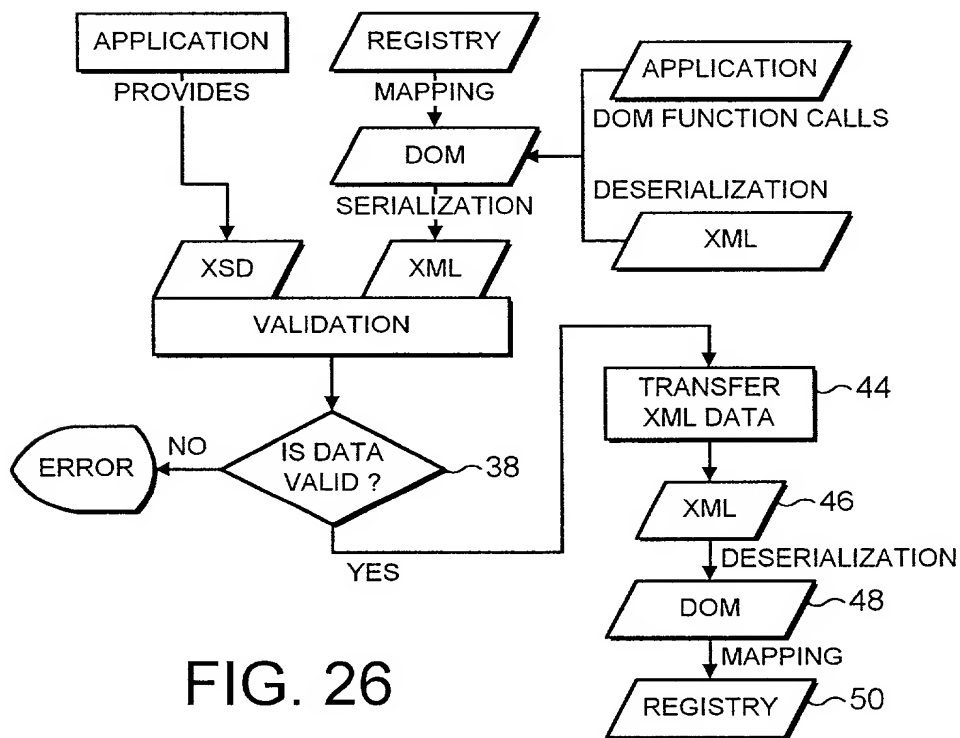


FIG. 26

20090242500

25 / 25

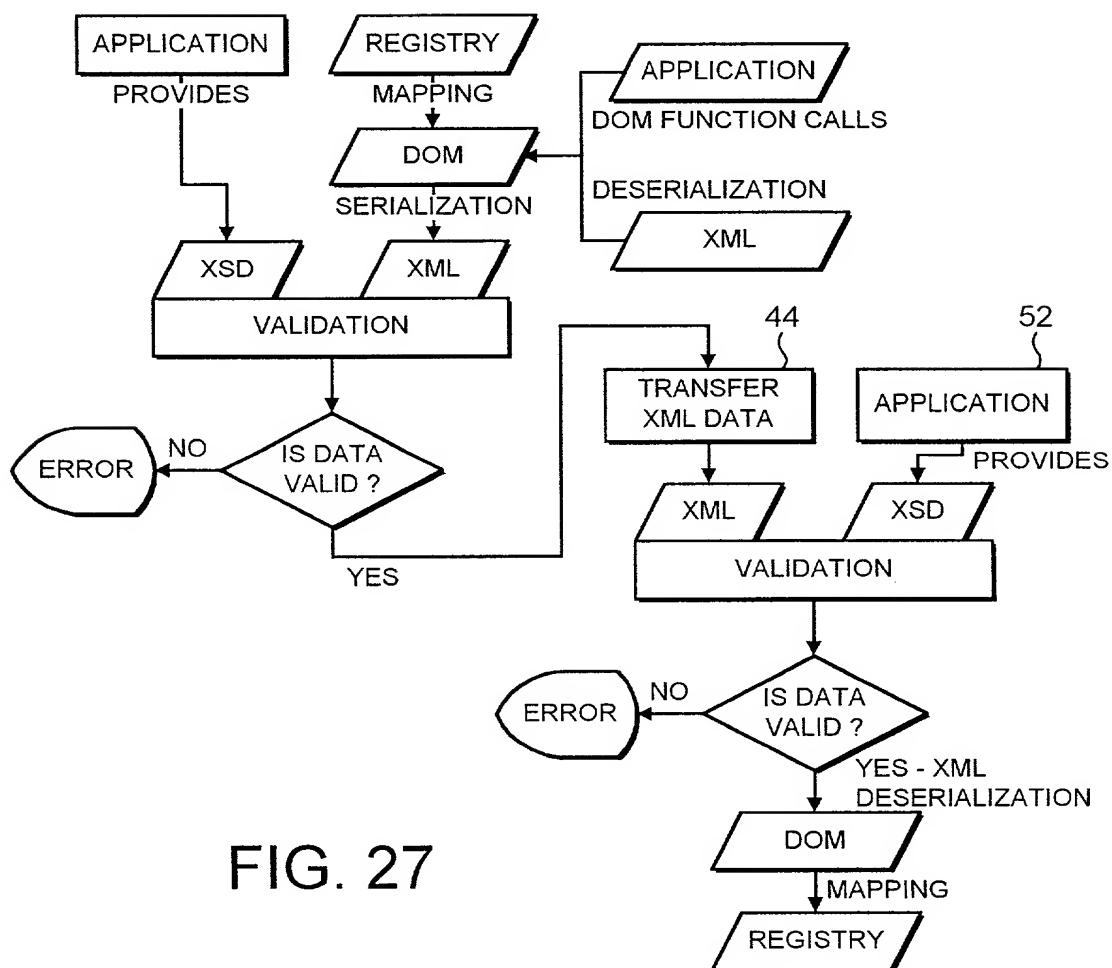


FIG. 27

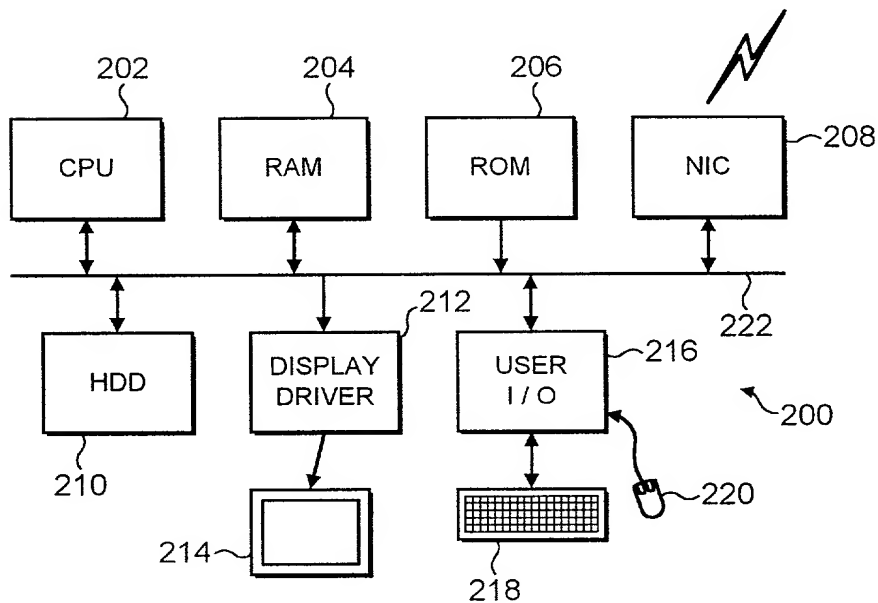


FIG. 28